Encrypting with BitLocker To Go for removable devices under Windows 10
(BitLocker To Go User Guide)

1. Introduction

BitLocker To Go—a feature of Windows 10—is a full-disk encryption protection technology for removable storage devices that are connected to one of the USB ports on your computer (referred as either USB drive or drive hereafter).

Basically, BitLocker To Go allows you to encrypt a USB drive and restrict access with a password. When you connect the encrypted USB drive to a Windows 10 computer, you will be prompted for the password and upon successfully entering it, you can read and write to the drive as usual.

2. Turning on BitLocker To Go for a USB Drive

i. Go to “This PC” and select the USB Drive you want to encrypt, right click and select “turn on BitLocker”.

ii. Once the initialization process is completed, BitLocker To Go will prompt you to set up a password that is used to unlock the drive.
iii. After setting up a password, BitLocker To Go will prompt you to store or print the recovery key that is used to unlock the drive, in case you forget the password one day.

iv. You will be prompted to start the encryption process.
v. During the encryption process, a progress monitor will be shown. The amount of time that it will take to complete the process varies, depending mainly on the size of your drive.
vi. Once the encryption is complete, BitLocker To Go displays a confirmation dialog box and a lock icon will be shown on the Drive.

3. **Accessing a BitLocker To Go encrypted drive in Windows 10**

When a BitLocker To Go encrypted drive is plugged in any Windows 10 system, a dialog window will appear, informing you that the drive is protected by BitLocker Drive Encryption and waiting for you to enter the password.
After typing the password and clicking the Unlock button, you will be able to access the drive and its content as usual.

4. Recovering the encrypted USB drive using BitLocker recovery key

If you forget the password of the encrypted drive, the BitLocker recovery key saved or printed in 2 (iii) above will help you unlock the drive and create a new password for the drive.

i. Plug the encrypted USB drive in Windows 10 and click “More options”

ii. Enter the BitLocker recovery key and click “Unlock”
iii. Enter the BitLocker recovery key and click “Unlock”

If you have saved the recovery key in a file, you can simply copy and paste it; otherwise, you have to enter the long key carefully.

iv. Click “This PC”, highlight the removable drive and right click “Manage BitLocker”
v. Click “Change password”

5. Forgetting both the password and the recovery key
If you forget your old password, click the “Reset a forgotten password” and then create a new password and then click finish.

If you have lost both the password and the recovery key, you will lose your data forever as you cannot unlock the drive. Therefore, you are recommended to memorize the password and keep the printed or saved recovery key in a safe place.